



Troubleshooting Security Issues with nGenius InfiniStream & Sniffer Analysis

Executive Summary

This solution brief will discuss how Sniffer® Analysis and the nGenius® InfiniStream® appliances from NetScout® Systems, Inc. can be leveraged to troubleshoot security issues that occur in today's modern IP networks. The nGenius InfiniStream appliance, deployed in strategic locations in an enterprise or government agency network, watches and records the traffic traversing the network, giving IT staff valuable details related to potential security problems. This paper will show how using Sniffer Analysis can augment an existing cyber security initiative with targeted and focused troubleshooting capabilities, which solution features are best suited for the task and how the nGenius InfiniStream appliance is central to any IT organizations' security plan.

Challenges Securing the Modern IP Network

Firewalls, anti-virus software, intrusion detection/prevention systems (IDS/IPS) and anomaly behavior systems are traditional measures of defense against security breaches and cyber security incidents, but have limitations that prevent complete troubleshooting of potential security issues affecting application performance. IDS/IPS systems are only as good as the content that is delivered to them. Signatures occasionally produce false negatives (i.e., miss an event) and often generate false positives (i.e., report an event that is not a security threat).

Typically, when an alert is triggered, traditional security tools lack both the original packet as well as the essential functionality to analyze and identify the nature of the event. Without seamless drill down into the actual packet data, security and network teams are unable to troubleshoot whether the packets are a match to a virus or worm signature or simply an undefined new business service. Delays in effective troubleshooting can extend an outage and expand the potential damage to the infrastructure, services and end users.

An extra level of problem analysis capability and visibility is necessary for IT organizations to gain accurate information and appropriate depth of protection. Specifically required is a packet flow-based troubleshooting solution with 24x7 packet capture and long-term storage to enable quick forensics analysis of potential security issues. Prompt remediation in these situations helps organizations and government agencies avoid catastrophic network degradations.

Augmenting an IDS/IPS with full packet capture, decode and replay capabilities delivers security operations teams essential forensic details not otherwise available to pinpoint attacks that may originate from:

- Rogue wireless devices
- Trojans or worms introduced via laptops, personal email services or Flash-based storage devices (e.g., USB drives)
- Zero-day attacks or known attacks for which signatures have not been implemented
- Unauthorized remote control "zombie" or peer-to-peer software

Delays in effective troubleshooting can extend an outage and expand the potential damage to the infrastructure, services and end users. Avoiding such damaging disruption is ultimately the IT organization's goal.

Selecting and Deploying the nGenius InfiniStream Appliance as a Defense Strategy

NetScout offers Sniffer Analysis software and the nGenius InfiniStream appliance to troubleshoot security issues when deployed in strategic locations in government agency or enterprise networks. The nGenius InfiniStream appliance fills the void typically faced by IDS/IPS systems by providing a solution for troubleshooting potential security issues affecting service delivery as it watches and records the traffic traversing the network, identifies potential issues and alerts IT staff of suspect threats.

The nGenius InfiniStream appliance is a high performance, highly available Linux-based appliance with intelligent Deep Packet Capture (iDPC) technology that provides post-mortem packet analysis by capturing network traffic 24x7 and storing it to disk for forensics analysis.

Sniffer Analysis is a software suite that provides forensic analysis and decodes across the nGenius InfiniStream packet store to speed troubleshooting and to minimize the impact of application performance issues and service degradations. Sniffer Analysis software includes:

- **The InfiniStream Console**--A software-based console providing a graphical, direct-connect interface for viewing summarized packet data and statistics residing on the appliance. It provides unrestricted mining of the entire data store across a wide array of criteria, allowing selection of exact conditions with which to launch into deeper analysis with Sniffer Intelligence or Sniffer decodes.
- **Sniffer Intelligence**--An automated application providing discovery and statistics to speed application analysis and problem resolution using a flexible and dynamic workflow. It leverages data captured by nGenius InfiniStream appliances.

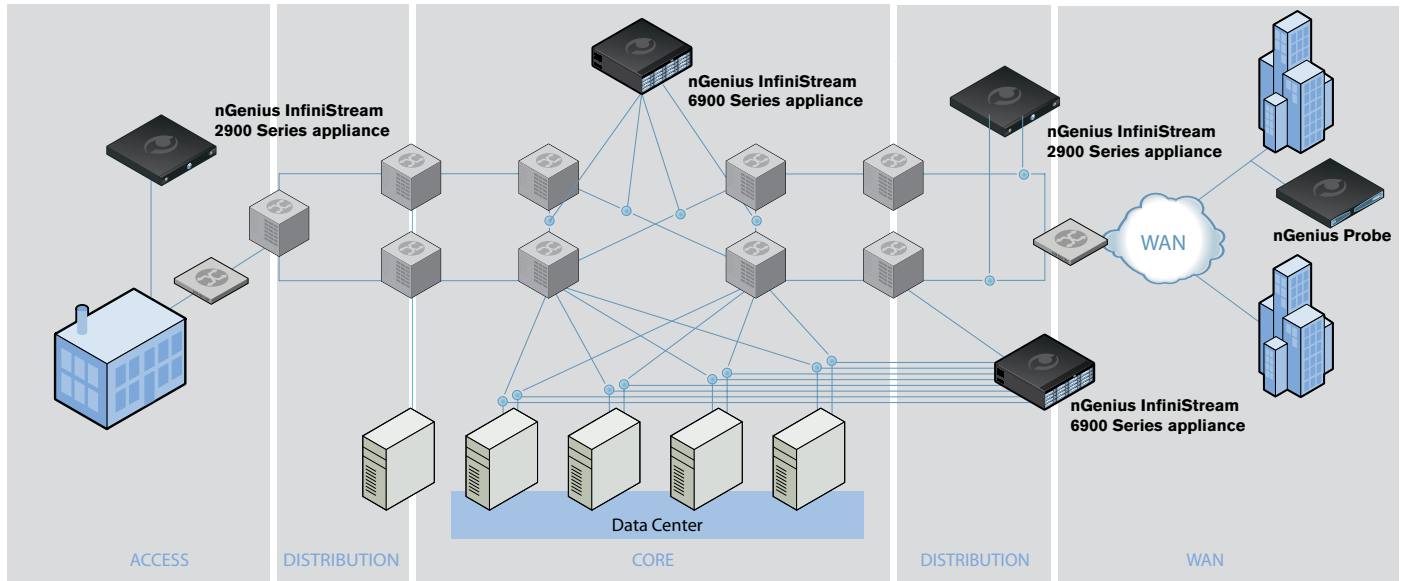


Figure 1: nGenius InfiniStream 2900 and 6900 series appliances strategically deployed in an enterprise network.

All nGenius InfiniStream models support Sniffer Analysis and are available in two different form factors for different deployment requirements: nGenius InfiniStream 2900 Series and nGenius InfiniStream 6900 Series. Selecting the right nGenius InfiniStream appliance for troubleshooting security issues will involve a variety of criteria:

- **Storage**--Range of storage capacity for continuous packet recording with intelligent Deep Packet Capture from 500 GB up to 16 TB of storage
- **Interfaces**--Several options for 10/100/1000 Base-T or Gigabit Ethernet SFP up to 10 Gigabit Ethernet configurable alternatives
- **Ports**--Variety of flexible 2, 4, or 8 port configuration choices
- **Implementation**--User configurable choices for dedicated tapping of key segments or to connect to switch analyzer ports (mirror ports) for port spanning

The following outlines unique characteristics of Sniffer Analysis and the nGenius InfiniStream appliance that supports troubleshooting of security issues.

Leverage intelligent Deep Packet Capture (iDPC) technology, a foundation of the nGenius InfiniStream appliance, maximizes storage capabilities using algorithms that balance overall drive storage with quick retrieval and resiliency. By employing multiple methods for efficient indexing of the stored metadata, users can troubleshoot security issues using efficient, contextual drill downs, to the single conversation or packet in question stored in the nGenius InfiniStream appliance. Technical elements of iDPC include:

- **Long-term, 24x7 packet capture and storage** for quick forensics analysis of potential security issues and rapid remediation; having the incident captured and recorded in its first instance reduces time to wait for the threat to reoccur and allows immediate troubleshooting to begin.

- **Smart Recording and Data Mining (SRDM) technology**, an essential element of iDPC, is a specialized data reduction and storage optimization approach that enables organizations to selectively record and store, on a per-application basis, all, none, or part of the packets of interest

Access via the InfiniStream Console as a direct-connect interface to the nGenius InfiniStream appliance serves as a launch point for back-in-time analysis. A traditional traffic-over-time display provides a thumbnail overview of monitored traffic that offers a trended view for the recent past.

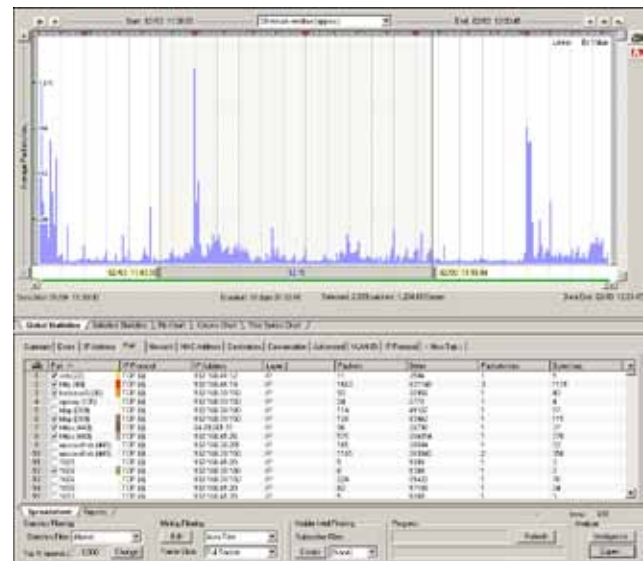


Figure 2: The InfiniStream Console offers a direct-connect interface to the nGenius InfiniStream appliance for back-in-time views and analysis.



Use on-board flexible filtering and data mining by building capture filters and custom rules to isolate and retrieve data from within the InfiniStream capture store to focus on any particular security threat. By refining the data set for analysis, by time, user, pattern or application associated with the security issue in question, the IT staff can accelerate problem resolution by focusing on the most important packets related to the event. An operator can create capture filters using any one or a combination of the following metrics:

- MAC and IP addresses
- TCP or UDP ports
- DNS names
- Protocols
- Hex, binary, or text patterns
- ToS (Type of Service)
- Time increments

The launch of Sniffer Intelligence, a post-capture expert analysis software solution within the nGenius InfiniStream appliance provides critical back-in-time voice and data analysis. With automatic recognition of hundreds of applications, such as SAP® R/3®, Oracle®, MS Exchange, and VoIP traffic, Sniffer Intelligence provides critical performance data to speed performance analysis and problem resolution. Once a selection of data is isolated within the InfiniStream Console, Sniffer Intelligence modules provide detailed forensics analysis of each type of application, incorporating a rich set of packet-flow statistic, charts, and graphs to simplify the analysis process. As even more details are required, Sniffer experts and decodes are available to translate complex technical jargon into plain English to better understand, troubleshoot, and tune potential security and performance issues.

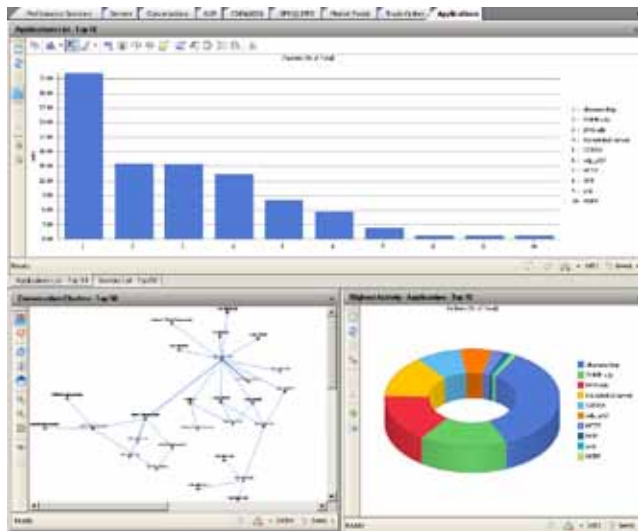


Figure 3. Sniffer Intelligence graphically represents data for quick troubleshooting analysis of security issues.

Pinpoint a New Security Vulnerability

Business Challenge: A new virus or worm had made its way into a government agency network by way of an employee-owned laptop. The agency's IT contractors need a way to track down systems that had already been impacted.

Solution: The nGenius InfiniStream appliance had been continuously capturing and storing packets from strategic segments in the affected building. The IT contractors built a post-capture filter that matched the signature of the virus. They ran the filter against the stored packets and found all the IP addresses of the networked workstations and laptops that were infected.

Business Result: Rapid identification of the infected systems enabled quick removal from the network and remediation of the virus from the affected equipment. In so doing, they avoided a broad dissemination of the virus network-wide that would have hindered the agency for the rest of the day or even several days.

Reduce False Positives

Business Challenge: The number of potential threats identified by an IDS/IPS system was becoming difficult to validate in a timely manner. The IT staff and security team were concerned about both the time lost on false positives and the potential for delay in identifying actual threats. They needed a way to rapidly research these incidents and then re-configure the IDS/IPS system to stop alerting on approved traffic.

Solution: The nGenius InfiniStream appliance was co-located with the IDS/IPS sensors and continuously captured and stored packets from those parts of the network. The IT team would use the reports from the IDS system to filter on the time-stamps around the suspect alerts and identify unknown traffic at the same time. Using the InfiniStream Console, the IT team performed expert analysis and packet decodes to definitively identify the packets by the correct protocols, applications, users and security status.

Business Result: With a systematic, repeatable process, the IT organization was able to take the information from the nGenius InfiniStream and re-configure the IDS/IPS sensors to allow the new applications launched by the development team to be passed through the network without alerts. This reduced the false positives and improved the productivity of the security team to be able to address actual threats more expeditiously.

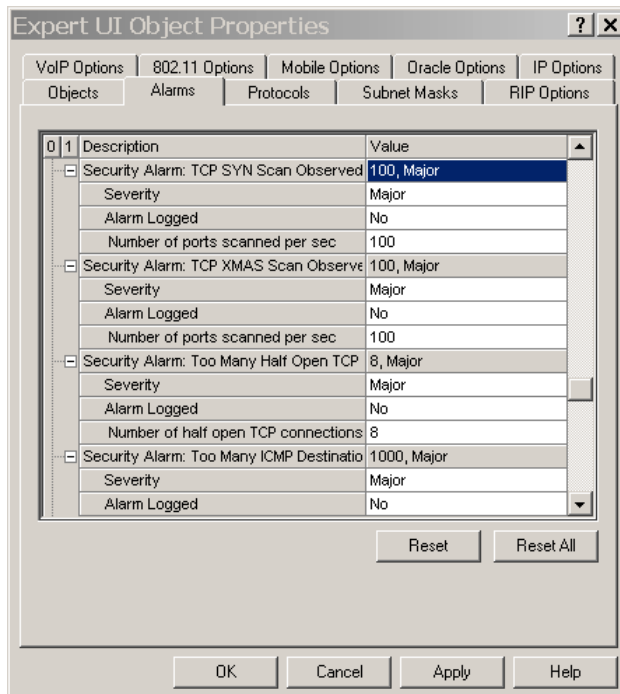


Figure 4: Using decode and expert analysis features in Sniffer Analysis helps quick identification and rapid remediation of a potential DOS attack.

Troubleshooting Potential Denial of Service Threat

Business Challenge: Users were reporting slowdowns when trying to connect to the data center from a regional office where more than 250 employees depended on the network to do their job every day. The IT organization needed to troubleshoot the slowdown and track a potential denial of service (DOS) threat. DOS and Distributed DOS (DDOS) attacks can make an Internet site or service unavailable to the intended users, thus creating significant disruption in business activity for those authorized users.

Solution: With the nGenius InfiniStream appliance continuously capturing and storing packets from the strategic segments at the regional office, the IT organization quickly identified an increase in traffic to the Internet. Decode and expert analysis functionality immediately flagged a major "TCP SYN Scan," a type of attack employed by hackers to uncover unprotected ports and compromise them. The attack was automatically detected hundreds of ports were being scanned at the regional office.

Business Result: Rapid identification of a potential DOS attack gives IT staff metrics and potential IP source information necessary to shut down the threat and avoid a catastrophic disruption in services.

Using the full complement of features and functions provided by Sniffer Analysis and the nGenius InfiniStream appliance, organizations are well armed to accelerate problem resolution of security issues as they may occur in today's modern IP networks.

nGenius InfiniStream as A Foundation for the nGenius Service Assurance Solution

The nGenius InfiniStream appliance works standalone, as described throughout this paper, or seamlessly incorporated into the more robust service delivery management system, the nGenius Service Assurance Solution. The nGenius Service Assurance Solution is a suite of products that can leverage data from multiple nGenius InfiniStream appliances, as well as other nGenius data sources such as nGenius Probes and nGenius Virtual Agents. The information gathered by the nGenius InfiniStream appliances is analyzed and viewed with nGenius K2 Service Delivery Manager and nGenius Performance Manager for a unified presentation of metrics collected from the various points across the network. In addition to addressing security issues with the forensic data mining capabilities of Sniffer Analysis, the nGenius Service Assurance Solution is used for intelligent early warning, application and network performance management, planning and optimization, and service and policy validation.

Conclusion

The NetScout nGenius InfiniStream appliances utilize iDPC technology to deliver real-time and back-in-time data mining to troubleshoot potential security issues that threaten efficient delivery of business services. Deployed in strategic locations in an enterprise or government agency network, the nGenius InfiniStream watches and records the traffic traversing the network, identifies potential issues, alerts IT staff, and enables rapid problem resolution of suspect issues. Sniffer Analysis software and nGenius InfiniStream appliances can augment an existing network security initiative with targeted and focused troubleshooting capabilities, and thus an essential element of any IT organizations' security assurance plan.

**Corporate Headquarters**

310 Littleton Road
Westford, MA 01886-4105
Phone: 978-614-4000
Toll Free: 888-999-5946
www.netscout.com

European Headquarters

NetScout Systems (UK) Ltd.
100 Pall Mall
London SW1Y 5HP
United Kingdom
Phone: +44 (0)20 7321 5660

Asia/Pacific Headquarters

Room 105, 17F/B, No. 167
TunHwa N. Road
Taipei, Taiwan
Phone: +886 2 2717 1999
www.netscout.cn

For More information

**For more information please visit
www.netscout.com or contact NetScout
sales at 800-309-4804 or +1 978-614-4000**

Copyright © 2010 NetScout Systems, Inc. All rights reserved. NetScout, the NetScout logo, nGenius, Sniffer and InfiniStream are all registered trademarks of NetScout Systems, Inc. All other registered and non-registered trademarks are the property of their respective owners.

SOES_02_2010 Rev A